УТВЕРЖДАЮ
Генеральный Директор
ООО «ИК «КОИН»

_____ / Близняк А.Б.

«01» февраля 2011 г.

ПОЛИТИКА
безопасности персональных данных ООО «Инвестиционная компания «КОИН»

Москва, 2011 г.

Оглавление

Введение

«Политика безопасности персональных данных» (далее – Политика) определяет стратегию защиты персональных данных, обрабатываемых в информационных системах персональных данных ООО «ИК «КОИН» и формулирует основные принципы и механизмы защиты персональных данных.

Политика является основным руководящим документом Организации, определяющим требования, предъявляемые к обеспечению безопасности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Настоящий документ разработан в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и на основании положений Стандарта НАУФОР «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг».

1. Общие положения

1.1. Цель и область применения политики

Целью Политики является обеспечение безопасности персональных данных, а также реализация положений нормативных правовых актов и иных документов по защите персональных данных.

Основными целями обеспечения безопасности персональных данных являются:

— предотвращение нарушений прав субъекта персональных данных (физического лица) на сохранение конфиденциальности информации, обрабатываемой в информационных системах персональных данных Организации;

— предотвращение искажения или несанкционированной модификации информации, содержащей персональные данные, обрабатываемой в информационных системах персональных данных Организации;

— предотвращение несанкционированных действий по блокированию информации, содержащей персональные данные.

Требования настоящей Политики обязательны для всех структурных подразделений Организации и распространяются на:

— автоматизированные системы Организации;

— средства телекоммуникаций;

— информационные ресурсы и носители информации;

— помещения;

— работников Организации.

Внутренние документы Организации, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Политики и не противоречить им.

1.2. Субъекты персональных данных:

— сотрудник Организации – субъект персональных данных, который является работником Организации на основании ТК РФ;

— клиент Организации – субъект персональных данных, который пользуется услугами Организации на основании договора;

— бывший сотрудник Организации (пенсионеры, уволенные сотрудники) – субъект персональных данных, более не состоящий в трудовых отношениях с Организацией.

1.3. Состав персональных данных

В информационных системах Организации происходит обработка, передача, накопление и хранение информации, содержащей персональные данные, которые, в соответствии с действующим законодательством Российской Федерации, подлежат защите.

1.3.1. В Организации определены следующие основания для обработки информации, содержащей персональные данные:

— Федеральный закон РФ от 27.07.06 № 152-ФЗ «О персональных данных»;

— постановление Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Глава 14 Трудового Кодекса РФ.

1.3.2. Цель обработки информации, содержащей персональные данные – осуществление Организацией своей основной деятельности в соответствии с Уставом.

1.3.3. В состав персональных данных работника входят:

— фамилия, имя, отчество (в т.ч. предыдущие);

— паспортные данные или данные документа, удостоверяющего личность;

— дата рождения, место рождения;

— гражданство;

— данные миграционной карты и/или иного документа, подтверждающего право Субъекта - иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации;

— отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения;

— данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке;

— данные документов о подтверждении специальных знаний;

— данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях;

— знание иностранных языков;

— семейное положение и данные о составе и членах семьи;

— сведения о социальных льготах, пенсионном обеспечении и страховании;

— данные документов об инвалидности (при наличии);

— данные медицинского заключения (при необходимости);

— стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке;

— должность, квалификационный уровень;

— сведения о заработной плате (доходах), банковских счетах, картах;

— адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства;

— номер телефона (стационарный домашний, рабочий, мобильный);

— сведения об отсутствии судимости - только в отношении круга лиц и в случаях, определенных законодательством;

— сведения об отсутствии дисквалификации - только в отношении круга лиц и в случаях, определенных законодательством;

— данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН);

— данные страхового свидетельства государственного пенсионного страхования;

— данные страхового медицинского полиса обязательного страхования граждан;

— иные персональные данные.

1.3.4. В состав персональных данных клиента входят:

1) анкетные и биографические данные, в т.ч.:

— фамилия, имя, отчество;

— дата и место рождения;

— гражданство;

— сведения о документе, удостоверяющем личность (вид, серия, номер, орган, выдавший документ, код подразделения, срок действия);

— сведения о наличии статуса иностранного публичного должностного лица;

— адрес (места жительства (регистрации), почтовый, места пребывания, фактического проживания);

— адреса средств связи (номера телефонов, факсов, электронные адреса);

— реквизиты счетов, в т.ч.: банковских, клиентских счетов в рамках договоров на брокерское обслуживание, счетов депо в рамках договоров на депозитарное обслуживание, счетов, открытых в рамках договоров доверительного управления, лицевых счетов, открытых для учета прав на инвестиционные паи;

— данные миграционной карты и/или иного документа, подтверждающего право Субъекта - иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации;

— сведения о присвоении ИНН;

2) сведения об имущественном положении, об имуществе и имущественных правах, находящихся в собственности, залоге, доверительном управлении, на основании иных прав, в т.ч.:

— сведения о денежных средствах на клиентских счетах в рамках договоров на брокерское обслуживание;

— сведения о ценных бумагах, в т.ч. паях инвестиционных фондов;

— сведения о ценных бумагах на счетах депо в рамках договоров на депозитарное обслуживание;

— сведения о размере и источниках доходов от договоров доверительного управления имуществом;

— сведения об участии в органах управления юридических лиц, в т.ч. в качестве единоличного исполнительного органа, в коллегиальном исполнительном органе, совете директоров (наблюдательном совете);

— сведения о размерах начисленного, удержанного и оплаченного НДФЛ;

— иные персональные данные.

2. Общие требования по организации защиты персональных данных

2.1. Организационная структура по обеспечению безопасности персональных данных

2.1.1. В целях выполнения задач по обеспечению безопасности персональных данных в Организации, в соответствии с рекомендациями российских стандартов по безопасности персональных данных, организационную структуру системы обеспечения безопасности персональных данных в Организации можно представить в виде совокупности следующих уровней:

— Первый уровень – Руководство Организации;

— Второй уровень – Уполномоченное лицо по обеспечению безопасности персональных данных и Системный администратор;

— Третий уровень – Сотрудник Организации.

2.1.2. Общее руководство системой обеспечения безопасности персональных данных осуществляет Генеральный Директор ООО «ИК «КОИН».

2.1.3. Уполномоченное лицо отвечает за:

— учет лиц, допущенных к работе с персональными данными в информационных системах;

— организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

— проведение разбирательств по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

— приостановку предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных.

2.1.4. Системный администратор отвечает за:

— администрирование информационных систем персональных данных;

— администрирование средств антивирусной защиты информационных систем персональных данных;

— администрирование средств и систем защиты персональных данных в информационных системах персональных данных.

2.1.5. Обработка персональных данных осуществляется работниками, имеющими допуск к персональным данным в соответствии с приказом Генерального Директора Организации. Данные работники обязаны соблюдать положения настоящей Политики, а также своих должностных инструкций и других документов Организации в области защиты персональных данных.

2.2. Требования к организационным мерам по обеспечению безопасности персональных данных

2.2.1. Основные положения

Основой организационных мероприятий по обеспечению безопасности персональных данных являются нормативные правовые акты и иные документы по защите персональных данных, в частности данная Политика. Данные документы определяют стратегию и требования по защите персональных данных. Положения данных документов доводятся до всех работников, ответственных за безопасность персональных данных.

Мероприятия по обеспечению безопасности персональных данных организуются и проводятся в соответствии с требованиями нормативных правовых актов:

— Федерального закона РФ от 27.07.06 № 152-ФЗ «О персональных данных»;

— Положения, утвержденного Постановлением Правительства РФ от 17 ноября 2007 г. «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Положения, утвержденного Постановлением Правительства РФ от 15 сентября 2008 г. «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

При обработке персональных данных субъектов персональных данных допущенные к ним работники Организации обязаны соблюдать следующие требования:

2.2.1.1. Организация не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, приведенных в п.2 ст.6 Федерального закона №152-ФЗ «О персональных данных». Письменное согласие субъекта персональных данных должно включать:

— фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

— наименование и адрес Организации;

— цель передачи персональных данных;

— перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

— перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Организацией способов обработки персональных данных;

— срок, в течение которого действует согласие, а также порядок его отзыва.

Типовая форма согласия для сотрудников приведена в Приложении №1, для клиентов – в Приложении №2.

2.2.1.2. В Организации запрещается обрабатывать специальные категории персональных данных, в том числе данные субъекта о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах.

2.2.1.3. Передача персональных данных субъектов третьей стороне не допускается без письменного согласия субъектов персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

2.2.1.4. В случае выявления недостоверных персональных данных субъекта персональных данных или неправомерных действий с ними работников Организации при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных, относящихся к соответствующему субъекту, с момента такого обращения или получения такого запроса на период проверки.

2.2.1.5. В случае подтверждения факта недостоверности персональных данных субъекта персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов производится уточнение персональных данных, соответствующая блокировка снимается.

2.2.1.6. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с момента выявления, Уполномоченное лицо обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с момента выявления неправомерности действий с персональными данными, Уполномоченное лицо обязано уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Уполномоченное лицо обязано уведомить субъекта персональных данных или его законного представителя, а в случае, если

обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомляется указанный орган.

2.2.2. Анализ угроз

Обеспечение безопасности персональных данных, а также разработка и внедрение системы защиты персональных данных основывается на анализе угроз безопасности персональных данных.

Системный администратор является ответственным за разработку и поддержку Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Частная модель угроз).

В качестве исходных данных для разработки Частной модели угроз в Организации используется Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных, введённая Стандартом НАУФОР «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг» (далее – Базовая модель угроз).

Частная модель угроз должна отражать актуальное состояние защищенности информационных систем персональных данных и актуальные угрозы безопасности персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемой информационной системе персональных данных.

2.3. Порядок действий в случае запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных

Ответственным за обработку запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, является Уполномоченное лицо.

Назначение Уполномоченного лица производится приказом Генерального Директора Организации. При поступлении запросов уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных, Уполномоченное лицо обязано:

— действовать в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ;

— уведомить Генерального Директора Организации о поступлении обращения субъекта персональных данных;

— подготовить ответ в соответствии с запросом уполномоченного органа по защите прав субъектов персональных данных или запросом иных надзорных органов, осуществляющих контроль и надзор в области персональных данных;

— направить соответствующий ответ в адрес уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

2.4. Порядок хранения отдельных материальных носителей персональных данных

2.4.1. Основные принципы хранения отдельных материальных носителей персональных данных:

— при фиксации персональных данных на материальных носителях не допускать фиксацию на одном материальном носителе персональных данных, цели обработки которых различны;

— для каждой категории персональных данных использовать отдельный материальный носитель;

— материальные носители, содержащие персональные данные, обработка которых осуществляется в различных целях, хранить раздельно (в отдельных шкафах (сейфах) или на отдельных полках);

— при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.5. Доступ в помещения, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных

2.5.1. Доступ в помещения, в которых ведётся обработка персональных данных, лицам, не являющимися работниками Организации, запрещён. Исключение составляют только работниками государственных органов, организаций, доступ в помещения которым разрешается в соответствии с нормативными правовыми актами.

Доступ названных лиц осуществляется с разрешения Генерального Директора Организации. При этом сотрудники государственных органов и организаций допускаются в помещения, в которых ведётся обработка персональных данных, только в сопровождении работников Организации, уполномоченных распоряжением (устным или письменным) Генерального Директора Организации для сопровождения конкретных лиц. При этом ознакомление сотрудников государственных органов, организаций, которые прибыли в помещения с сопровождающим, с обрабатываемыми персональными данными не допускается.

2.5.2. Доступ в помещения, в которых размещаются средства обработки и/или защиты персональных данных, разрешён только работникам, непосредственно занятым обработкой персональных данных или обслуживанием информационных систем персональных данных (систем защиты персональных данных).

Перечень работников, непосредственно занятых обработкой персональных данных или обслуживанием информационных систем персональных данных (систем защиты персональных данных) устанавливается приказом Генерального Директора Организации.

Другие работники Организации, непосредственно не занятые в обработке персональных данных или обслуживании информационных систем персональных данных (систем защиты персональных данных), а также работники других организаций (в т.ч. сотрудники государственных органов) допускаются в помещения, в которых размещаются средства обработки и/или защиты персональных данных, только в сопровождении работников, уполномоченных приказом Генерального Директора Организации на обработку персональных данных или обслуживание информационных систем персональных данных (систем защиты персональных данных). При этом ознакомление лиц, которые прибыли в помещения с сопровождающим, с обрабатываемыми персональными данными не допускается.

2.5.3. Общие требования к доступу в помещения, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных

Требования настоящего раздела являются обязательными на всех стадиях проектирования, строительства, оснащения и эксплуатации помещений, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных (далее - Помещения).

Помещения должны размещаться в пределах контролируемой зоны. При этом рекомендуется размещать их на максимальном удалении от границ контролируемой зоны, чтобы ограждающие конструкции (стены, полы, потолки) не являлись смежными с помещениями, расположенными на неохраняемой территории.

Целесообразно, чтобы окна выходили на закрытую для несанкционированного доступа территорию, имели шторы (жалюзи).

Эффективность защиты Помещений должна соответствовать требованиям нормативных правовых актов и иных документов по обеспечению безопасности персональных данных.

Достаточность предпринятых мер защиты Помещений, а также необходимость дополнительных мер защиты определяются при периодических проверках Помещений.

2.5.4. Организационно-режимные требования к помещениям, в которых ведётся обработка персональных данных, и/или размещаются средства обработки персональных данных, и/или хранятся носители персональных данных

2.5.4.1. Для Помещений, в которых ведётся обработка персональных данных, необходимо выполнять следующие требования:

— двери Помещений необходимо оборудовать замками повышенной надежности;

— выдача ключей от Помещений должна производиться лицам, работающим в нем или ответственным за это помещение;

— уборка этих Помещений должна производиться в присутствии лиц, ответственных за эти помещения, или специально выделенными уборщицами;

— в случае ухода из этих Помещений в рабочее время необходимо их закрывать на ключ или оставлять под ответственность доверенных лиц (например, секретаря).

2.5.4.2. В случае обнаружения факта несанкционированного проникновения в Помещения должно производится расследование.

3. Пресечение (устранение) нарушений установленных норм и требований по обеспечению безопасности персональных данных

Своевременное и оперативное пресечение (устранение) нарушений норм и требований по обеспечению безопасности персональных данных является важнейшим требованием сохранения конфиденциальности персональных данных.

Невыполнение предписанных мер по обеспечению безопасности персональных данных считается предпосылкой к нарушению конфиденциальности персональных данных (далее - предпосылка).

По каждой предпосылке немедленно докладывается Генеральному Директору Организации для выяснения обстоятельств и причин невыполнения установленных требований, а также проводится расследование.

Для проведения расследования по приказу Генерального Директора Организации назначается комиссия из компетентных лиц. Комиссия обязана установить, имелось ли нарушение конфиденциальности персональных данных. После окончания расследования принимаются меры по устранению нарушений.

Работники, организующие и осуществляющие обработку и/или защиту персональных данных, обязаны строго соблюдать требования по защите персональных данных и несут ответственность за нарушения, приводящие к нарушению конфиденциальности персональных данных.

Нарушения норм и требований по обеспечению безопасности персональных данных делятся на три категории:

а) нарушение первой категории:

невыполнение норм и требований по обеспечению безопасности персональных данных, в результате которого произошло нарушение конфиденциальности персональных данных;

По всем случаям нарушений первой категории немедленно докладывается Генеральному Директору Организации.

б) нарушение второй категории:

невыполнение норм и требований по обеспечению безопасности персональных данных, в результате которого имелась или имеется реальная возможность нарушения конфиденциальности персональных данных;

в) нарушение третьей категории:

невыполнение других требований по обеспечению безопасности персональных данных, не приводящих к нарушениям первой и второй категорий.

О нарушениях второй и третьей категорий докладывается Заместителю Генерального Директора Организации. По указанию Заместителя Генерального Директора Организации немедленно организуется пресечение нарушения, выявляется причина допущенного нарушения, оценивается степень возможного ущерба и принимаются меры к его устранению.

4. Техническая защита персональных данных

4.1. Общие положения

Для защиты персональных данных, обрабатываемых в Организации, внедрена система защиты персональных данных – комплексная система, позволяющая обеспечить конфиденциальность персональных данных, хранящихся и обрабатываемых в Организации.

Внедрение или модернизация система защиты персональных данных представляет собой поэтапный процесс, учитывающий особенности имеющейся информационной системы персональных данных, и включает в себя следующие этапы:

— предпроектное обследование информационной системы персональных данных;

— определение требований к системе защиты персональных данных;

— проектирование системы защиты персональных данных;

— создание системы защиты персональных данных.

Обоснование комплекса мероприятий по обеспечению безопасности персональных данных в информационных системах персональных данных Организации производится с

учетом результатов оценки опасности угроз и определения класса информационных система персональных данных на основе Приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» или положений Стандарта НАУФОР.

Защита персональных данных обеспечивается на всех технологических этапах передачи, обработки и хранения персональных данных и при всех режимах работы информационной системы персональных данных, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе меры (механизмы) защиты от НСД не должны ухудшать основные функциональные характеристики информационной системы персональных данных.

4.2. Состав системы защиты персональных данных

4.2.1. Система защиты персональных данных Организации включает в себя следующие подсистемы:

— Подсистема управления доступом. Подразумевает защиту информационных ресурсов Организации от несанкционированного доступа. Средствами подсистемы реализуются функции по управлению доступом пользователей к ресурсам, включая сетевые подключения и доступ к внешним носителям информации и устройствам.

— Подсистема управления учетными записями. Подразумевает защищенное централизованное управление учетными записями пользователей. Включает предоставление пользователю ролей для доступа к различным системам, а также проверку и корректировку избыточности прав пользователей. В рамках данной подсистемы реализуется централизованное управление средствами защиты информации, включающее управление обновлениями, а также уведомление администраторов об инцидентах информационной безопасности.

— Подсистема регистрации и учета. Подразумевает защиту информационных ресурсов Заказчика от несанкционированного доступа. Средствами подсистемы реализуется регистрация и учет действий пользователей в различных системах, что позволяет, например, зафиксировать факты обращения пользователей к конфиденциальным ресурсам.

— Подсистема криптографической защиты. Обеспечивает защиту данных при хранении и передаче по каналам связи. Подсистема может включать в себя средства формирования ЭЦП.

— Подсистема защиты от вредоносного кода и спама. Обеспечивает защиту от вредоносного кода, получаемого по электронной почте, сети Интернет, другим каналам, а также защиту рабочих станций и серверов. Предоставляет защиту электронной почты от нежелательной корреспонденции.

— Подсистема обеспечения сетевой безопасности. Предотвращает возможные атаки, реализуемые на сетевом уровне. Включает в себя средства межсетевого экранирования, организации защищенных виртуальных сетей (включая удаленных пользователей), а также средства обнаружения и предотвращения вторжений.

— Подсистема межсетевого экранирования, которая обеспечивает защиту корпоративной сети передачи данных от внешних сетевых атак, а также защиту критичных внутренних сегментов сети, от действий внутреннего злоумышленника.

— Подсистема антивирусной защиты, которая помогает эффективно решать проблему защиты информационной системы от компьютерных вирусов. Надежность

подсистемы антивирусной защиты определяется не только технологическими достижениями, реализованными в антивирусных программах, но также комплексом организационных мер, направленных на их эффективное применение.

4.2.2. Средства защиты информации, применяемые в информационной системе персональных данных должны в установленном порядке проходить процедуру оценки соответствия (или иметь разрешение Генерального Директора Организации).

Для функционирующих информационных систем персональных данных доработка (модернизация) системы защиты персональных данных должна проводиться в случае, если:

— изменился состав или структура самой информационной системы персональных данных или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки персональных данных, топологии информационной системы персональных данных);

— изменился состав угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных;

— изменился класс информационной системы персональных данных.

5. Ответственность за соблюдение положений Политики

5.1 Общее руководство обеспечением безопасности персональных данных Организации осуществляет Генеральный Директор Организации.

5.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента безопасности персональных данных в Организации лежит на Уполномоченном лице.

5.3. Нарушение требований локальных нормативных актов Организации по обеспечению безопасности персональных данных является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между Организацией и сотрудниками, договорами, заключенными между Организацией и клиентами, и договорами, заключенными между Организацией и контрагентами.

5.4. Степень ответственности за нарушение требований локальных нормативных актов в области безопасности персональных данных определяется, исходя из размера ущерба, причиненного субъекту персональных данных.

5.5. Виды ответственности, предусмотренные отдельными федеральными законами об обращении с информацией ограниченного доступа:

— Гражданско-правовая ответственность;

— Дисциплинарная ответственность;

— Уголовная ответственность;

— Административная ответственность.

6. Контроль за соблюдением положений Политики

6.1. Общий контроль состояния безопасности персональных данных Организации осуществляется Генеральным Директором Организации.

6.2. Текущий контроль соблюдения положений настоящей Политики осуществляет Уполномоченное лицо.

7. Заключительные положения

7.1. Настоящая Политика вступает в силу с момента ее утверждения Генеральным Директором Организации и действует бессрочно до замены ее новой Политикой безопасности персональных данных.

7.2. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Организации, которые дополняют и уточняют ее.

7.3. Внесение изменений в Политику может быть вызвано изменениями в информационной системе персональных данных, системе защиты персональных данных, изменениями нормативных правовых актов и иных документов.

7.4. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Организации настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Организации. В этом случае Уполномоченное лицо обязано незамедлительно инициировать внесение соответствующих изменений.

7.5. Внесению изменений в Политику предшествуют:

— обследование и анализ изменений в информационной системе персональных данных, системе защиты персональных данных и/или;

— анализ изменений нормативных правовых актов и иных документов.

По завершении вышеназванных процедур анализа и обследования вносятся изменения (дополнения, исключения, новые редакции) в данную Политику обеспечения безопасности персональных данных;

7.6. Введение в действие новых редакций Политики осуществляется согласно процедурам документооборота, установленным в Организации.

7.7. Ответственным за внесение изменений в настоящую Политику является Уполномоченное лицо.

Приложение №1

СОГЛАСИЕ
РАБОТНИКА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____
(ф.и.о. работника)
зарегистрированный (ая) по адресу:_____

паспорт серия _____ № _____, выдан_____

_____ в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О защите персональных данных» даю согласие на обработку своих персональных данных ООО «ИК «КОИН», расположенному по адресу: 127055, г. Москва, ул. Новослободская д. 50/1, офис 12, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона № 152-ФЗ со всеми данными, которые находятся в распоряжении ООО «ИК «КОИН» с целью начисления заработной платы, исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления организацией-работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС РФ, сведений в ФСС РФ, предоставления сведений в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, а также предоставления сведений в случаях, предусмотренных федеральными законами и иными нормативно-правовыми актами, следующих моих персональных данных:

1. Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество (в т.ч. предыдущие);
- паспортные данные или данные документа, удостоверяющего личность;
- дата рождения, место рождения;
- гражданство;
- отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения;
- данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке;
- данные документов о подтверждении специальных знаний;
- данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях;
- знание иностранных языков;
- семейное положение и данные о составе и членах семьи;
- сведения о социальных льготах, пенсионном обеспечении и страховании;
- данные документов об инвалидности (при наличии);
- данные медицинского заключения (при необходимости);
- стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке;
- должность, квалификационный уровень;
- сведения о заработной плате (доходах), банковских счетах, картах;
- адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства;
- номер телефона (стационарный домашний, рабочий, мобильный);

— данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН);
— данные страхового свидетельства государственного пенсионного страхования;
— данные страхового медицинского полиса обязательного страхования граждан.

2. Перечень действий, на совершение которых дается согласие:

Разрешаю ООО «ИК «КОИН» производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

3. Сроки обработки и хранения персональных данных:

Обработка персональных данных прекращается после окончания трудового договора работника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении, а персональные данные работников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует с «____» _____г.

_____/ф.и.о. работника/ «____»_____г.
(подпись) (дата подписи)

Приложение №2

Генеральному директору ООО «ИК «КОИН»
от_____
(Ф.И.О.)

Согласие на обработку персональных данных

В соответствии с требованиями Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных» я, _____,
(Ф.И.О.)
паспорт _____ выдан_____
(серия, номер) (наименование органа, выдавшего документ)
адрес регистрации: _____
даю свое письменное согласие Обществу с ограниченной ответственностью «Инвестиционная компания «КОИН» на обработку моих персональных данных в целях исполнения Договора доверительного управления № _____, от «____» _____ 20___ года, а также исполнения требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Настоящее согласие не устанавливает предельных сроков обработки данных.
Я уведомлен и понимаю, что под обработкой персональных данных подразумевается сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), предоставление (в том числе передачу), уничтожение и любые другие действия (операции) с персональными данными.
Порядок отзыва согласия на обработку персональных данных мне известен.

_____
(Ф.И.О. полностью, подпись)

«___» _____ 201__ г.

Приложение №3

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных работников ООО «ИК «КОИН»

Я, _____, паспорт серии _____,номер_____,выдан_____ _____ « ___ » _____ года, понимаю, что получаю доступ к персональным данным работников ООО «ИК «КОИН».

Я также понимаю, что при исполнении своих обязанностей занимаюсь обработкой персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам Организации, как прямой, так и косвенный.

В связи с этим обязуюсь при работе с персональными данными работника соблюдать все требования, установленные «Политикой безопасности персональных данных».

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты, я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.

_____

(подпись, ФИО)

« ___ » _____ 201 ____ г.

Прошито, пронумеровано и скреплено печатью
(девятнадцать — 11 —) листа(-ов)
ООО «ИК «КОИН»
Генеральный директор Близняк А.Б.